

## UNITED STATES DISTRICT COURT

for the

Eastern District of Pennsylvania

United States of America

v.

Joshua Brioso

Case No. 19-176

Defendant(s)

## CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of 4/3/17 - 7/18/18 in the county of Bucks in the  
Eastern District of Pennsylvania, the defendant(s) violated:

Code Section

Offense Description

18 U.S.C. § 2252A(g)

Engaging in Child Exploitation Enterprise.

This criminal complaint is based on these facts:

See attached affidavit.

☒ Continued on the attached sheet.


Complainant's signature

Daniel J. Johns, Special Agent, FBI

Printed name and title

Sworn to before me and signed in my presence.

Date: 02/01/2019City and state: Philadelphia, Pennsylvania


Judge's signature

Hon. Elizabeth T. Hey, U.S. Magistrate Judge

Printed name and title

**AFFIDAVIT**

I, Daniel J. Johns, being first duly sworn, hereby depose and state as follows:

1. I am employed as a Special Agent of the Federal Bureau of Investigation (FBI) in Philadelphia, Pennsylvania. I am thus a “federal law enforcement officer,” as defined by the Federal Rules of Criminal Procedure. I have been employed as a Special Agent since March 2007. I am presently assigned to the Philadelphia Division’s Crimes Against Children squad, which investigates sex trafficking of children and prostitution investigations, child pornography, and kidnappings, among other violations of federal law. I have gained experience through training at the FBI Academy, various conferences involving crimes against children, and everyday work related to conducting these types of investigations.

2. This affidavit is being made in support of the issuance of the attached criminal complaint charging JOSHUA BRIOSO with engaging in a child exploitation enterprise, in violation of Title 18, United States Code Section 2252A(g).

3. The statements in this affidavit are based in part on my investigation of this matter and on information provided by other law enforcement officers. Because this affidavit is being submitted for the limited purpose of demonstrating probable cause in support of issuance of the attached complaint, I have not included each and every fact known to me concerning this investigation, but rather only those facts that I respectfully submit are necessary in order to establish probable cause.

**STATUTORY AUTHORITY**

4. Title 18, United States Code, Section 2252A(g) prohibits any person from engaging in a child exploitation enterprise. In turn, Title 18, United States Code, Section 2252A(g)(2)

provides that a person engages in a child exploitation enterprise within the meaning of the section if the person violates (among other portions of Title 18) Chapter 110 of the United States Code, as part of a series of felony violations constituting three or more separate incidents and involving more than one victim, and commits those offenses in concert with three or more other persons. Chapter 110 of the United States Code prohibits, among other offenses, the production of child pornography (18 U.S.C. § 2251(a)); the advertisement of child pornography (18 U.S.C. § 2251(d)); the distribution or receipt of child pornography (18 U.S.C. § 2252(a)(2)); and the possession of child pornography (18 U.S.C. § 2252(a)(4)(B)). Each of the aforementioned violations is a felony offense.

#### **PROBABLE CAUSE**

5. On or about May 23, 2017, an FBI online covert employee (OCE) was investigating the production of child pornography on the mobile app “live.me”<sup>1</sup> and browsed to a website called “8ch.net.” On 8ch.net, the OCE observed a link to a URL permitting browser-based access to Service A, a computer-based communication service described further below. Next to the link was an image that depicted two females who appeared to be children wearing bikinis.

6. The OCE clicked on the above link and was re-directed to another URL to a website operated by Service A-2. This particular website was entitled “Service A-1,” and the title was accompanied by a thumbnail image of two minor female children kissing each other.

---

<sup>1</sup> Live.me is a social media platform for sharing, creating and viewing live streaming videos. Live.me users can stream live video from mobile platforms like Apple iOS or Google Android. Videos streamed from Live.me users can be viewed through the Live.me mobile applications or an internet browser.

<sup>2</sup> Service A, Service A-1, and similar terms, as well as Username 1 and similar terms, are pseudonyms used in this affidavit in lieu of the actual terms in order to protect the integrity of an ongoing investigation.

7. Service A owns and operates a free-access all in one voice and text chat application and website with the same name that can be accessed over the web. A user creates a Service A account and can then communicate with other Service A users.

8. Service A users can exchange private messages between each other, participate in chat discussions, and voice chat. Service A users can also create chat rooms, which functions as message boards that can be accessed only by Service A users who have an invitation link. Service A-1, mentioned above, is one such chat room on Service A. Within these chat rooms, users can set up different sub-rooms wherein users can type written text, including links to files stored on external file-storage sites, and also upload files under a particular size limit, which can be viewed by all users of the sub-room. Service A users can share files larger than the limit allowed by providing hyperlinks to file sharing websites. Service A chat rooms can have one or more moderators. Moderators have the ability to manage other users, including but not limited to removing users from the chat rooms, elevating users hierarchically, and granting users additional permissions. The moderators of a chat room can categorize users of the chat rooms into hierarchical groups with customized labels and can configure those groups to give users in each group different levels of access.

9. The OCE's review of the Service A-1 chat room revealed that the vast majority of its content consisted of discussions about using web cameras and social-media applications to obtain sexually-explicit images and videos of minor children; images and videos of minor children exposing their vaginas, which at times were uploaded to the Service A-1 chat room and its sub-rooms; and links to download child pornography images and videos from external file-storage sites. Most of the children viewed by the OCE appeared to be approximately between the ages of 11 and 17 years old. The Service A-1 page also included some discussion of adults engaging in

sexual activity via web camera. However, the majority of the activity focused on the depiction of minors engaged in sexually explicit activity on web cameras. For example, in the course of a discussion in one sub-room of Service A-1 regarding the merits of utilizing virtual private network (VPN) technology to mask users' IP address and identity, Username 1 commented on April 15, 2017: "Just the fact that we're all hanging in here, which is a chatroom where underaged sexual content is shared around is enough reason for one to get a VPN." Username 1 continued: "Fuck when you download something from dropfile Your ISP can see what you downloaded What if govt authorities read ISPs logfiles."

10. Based on the OCE's undercover observations on Service A-1, a federal search warrant was issued on or about July 10, 2017, by the Honorable David R. Strawbridge, United States Magistrate Judge, Eastern District of Pennsylvania, for content stored on Service A's servers related to Service A-1. In response to the search warrant, Service A disclosed to law enforcement officers IP address information for some users of Service A-1, the content of some text chats occurring on Service A-1, and some private messages sent by users of Service A-1.

11. The Service A-1 chat room was ultimately shut down by Service A. Members of the Service A-1 chat room proceeded to open additional similar chat rooms on Service A, including: Service A-2, Service A-3, Service A-4, and Service A-5. The OCE gained access to Service A-3, Service A-4, and Service A-5. The OCE observed each of these chat rooms contained many of the same users as Service A-1 and were operated for the purpose of discussing, obtaining, and distributing child exploitation material including child pornography files. Service A-5 is the only of the aforementioned Service A chat rooms that is still operating.

12. Based on the OCE's undercover observations on Service A-2, Service A-3, Service A-4, and Service A-5, a second federal search warrant was issued on or about November 17, 2017,



by the Honorable Linda K. Caracappa, Chief United States Magistrate Judge, Eastern District of Pennsylvania, for content stored on Service A's servers related to the aforementioned chat rooms. In response to the search warrant, Service A disclosed to law enforcement officers IP address information for some users of those chat rooms, the content of certain text chats occurring in the chat rooms, and some private messages sent by users of those chat rooms.

13. The OCE observed a user of Service A-1 using the online names "Username 8" and "Username 9." A review of the search warrant return from Service A and undercover recordings by the OCE revealed, among other activity, the following activity, each involving a video that I have reviewed and that, in my opinion, constitutes a depiction of a minor engaged in sexually explicit conduct as defined by federal law:

a. On April 3, 2017, Username 8 posted a link on Service A-1 to material stored on Mega.nz – a file-storage site. By following the link, the OCE downloaded multiple files inside a folder entitled "4/2/17 Drops," including a file depicting a minor female exposing her vagina and masturbating.

b. On April 4, 2017, Username 8 posted another link on Service A-1 to material stored on Mega.nz. By following the link, the OCE downloaded a file depicting a minor female exposing her vagina.

c. On April 23, 2017, Username 8 posted another link on Service A-1 to material stored on Mega.nz. By following the link, the OCE downloaded multiple folders that contained approximately 30 videos depicting teenage girls, including apparent minors, in various stages of undress, sometimes exposing their genitals and masturbating.

d. Also on April 23, 2017, Username 8 posted a link on Service A-1 to a video file. The video associated with that link was found on a co-conspirator's computer, and it depicts

three prepubescent girls who appear to be 10 to 11 years old. At least one of the girls exposes her genitals to the camera.

e. On October 19, 2017, Username 9 posted information identifying a particular video from live.me on Service A-5. The OCE used that information to download a video depicting a minor female who appears to be 11 to 13 years old engaging in masturbation.

14. Records from Service A show that Username 8 and Username 9 accessed Service A from a particular IP address serviced by Charter Communications, and providing Internet access to 3753 E. Avenue 1 SPC 119, Lancaster, CA 93535 – BRIOSO's residence.

15. On July 18, 2018, a federal search warrant was executed at BRIOSO's residence in Lancaster, California. Law enforcement seized multiple digital devices belonging to BRIOSO, including a custom-built desktop computer with two hard drives and two cellular phones (an Apple iPhone X and a Samsung Galaxy S7). A forensic examination of the hard drives contained inside the desktop computer revealed the presence of approximately fifteen (15) videos depicting child pornography, including (but not exclusively) child pornography videos of the type frequently exchanged by members of the Discord enterprise (i.e., videos of apparent pre-teen minors and teenage minors originally streamed via web camera over online video-streaming services).

16. The examination further revealed that Service A had been downloaded onto the computer and had been frequently accessed by the user of the computer, as well as access to the e-mail account that had been used to register Username 8 and Username 9 with Service A. Particular software frequently used by members of the enterprise to download child pornography videos from one of the video streaming services had been installed, as had VPN software and hard drive wiping software. Evidence of having browsed to 28 separate links of the type commonly used in the enterprise to disseminate child pornography was recovered from BRIOSO's browser. Tor browser

activity was also located, including the submission of the search terms “pedo,” “14yo,” “8yo sucking,” and other similar terms. Finally, 37 records of visits to the website Mega (including download hyperlinks) were recovered (significant because Username 8 posted links to Mega storage sites containing child pornography over Service A-1, including in the links described specifically above).

17. Forensic analysis of the iPhone X revealed evidence that Service A had been downloaded and installed as an application, as well as the use of the e-mail address of record for Username 8 and Username 9 with Service A. The phone was further found to contain two images appearing to have been captured as screen shots from a video- and image-sharing application, depicting a minor female, apparently between the ages of 12 and 15, exposing her vagina to the camera. Also recovered were several text-message exchanges between BRIOSO and multiple apparent minor females (identification of whom is ongoing), some of which referenced sexual activity having taken place between BRIOSO and the minor. Some of these victims made explicit reference to their ages (13 and 15 years old) in recovered chats with BRIOSO.

18. BRIOSO was present at the residence when law enforcement arrived to execute the search warrant. He told the agents that he lived in the residence with his sister and father. He admitted to using Service A, but denied being familiar with Service A-1, Service A-5, Username 8, and Username 9. He denied using the internet to access child pornography. He also refused to provide agents with the PIN to access his iPhone but did give them consent to assume his online identity for his Gmail and Dropbox accounts.

### VENUE

19. The child exploitation enterprise in which BRIOSO engaged, as described above, extended at all relevant times to the Eastern District of Pennsylvania. The enterprise was open to

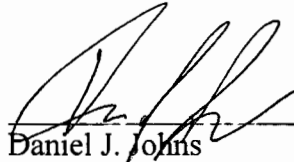


members from anywhere in the world, and the child pornography material disseminated by the enterprise was made available to any person able to access Service A, including from the Eastern District of Pennsylvania. Further, the OCE's activities over the various Service A chat rooms comprising the enterprise were conducted in the Eastern District of Pennsylvania. Finally, the investigation has revealed the participation of at least one member of the enterprise who lived in the Eastern District of Pennsylvania and participated in the enterprise from the Eastern District of Pennsylvania, from as early as July 2016 until that member's arrest by federal authorities in February 2018 pursuant to a complaint charging him with engaging in a child exploitation enterprise, in violation of 18 U.S.C. § 2252A(g).

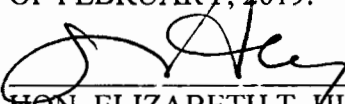
#### **CONCLUSION**

20. Based upon the information above, I respectfully submit that there is probable cause to believe that JOSHUA BRIOSO engaged in a child exploitation enterprise, in violation of Title 18, United States Code Section 2252A(g), in that BRIOSO violated Chapter 110 of Title 18 of the United States Code as part of a series of felony violations involving three or more separate incidents and more than one victim, as outlined in paragraph 13 of this affidavit, and has committed

those offenses with three or more other persons. I therefore further respectfully request that the Court approve the attached arrest warrant charging JOSHUA BRIOSO with that offense.

  
\_\_\_\_\_  
Daniel J. Johns  
Special Agent, Federal Bureau of Investigation

SWORN TO AND SUBSCRIBED  
BEFORE ME THIS 1<sup>st</sup> DAY  
OF FEBRUARY, 2019.

  
\_\_\_\_\_  
HON. ELIZABETH T. HEY  
UNITED STATES MAGISTRATE JUDGE